CLAIMS:

1. A method of processing a message for authentication, said method comprising:

performing a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function; and

using a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function.

2. The method of claim 1 wherein said step of using comprises the steps of:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using said second portion and said result as inputs.

3. The method of claim 2 wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

4. The method of claim 2 wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

5. The method of claim 1 further comprising the steps of:

using a result from said compression function to produce a message authentication code; and

sending said message authentication code in association with said message for authenticating said message using said message authentication code.

6. The method of claim 1 further comprises:

using a result from said compression function to produce a message authentication code; and

comparing said message authentication code to a received message authentication code received with said message, whereby said message is authentic if said message authentication code and said received authentication code match.

7. A method of processing a message for authentication, said method comprising:

providing a first portion and a second portion of said message;

performing a hash function using said first portion as an input to achieve a result; and

performing a keyed hash function using said second portion and said result as inputs.

8. The method of claim 7 comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing said steps of providing, performing and performing when said message does not fit within an input block of said compression function.

9. The method of claim 7 comprising the step of:

determining whether said message fits within an input block of a compression function; and

performing a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function.

10. The method of claim 7 wherein said hash function is an iterated hash function F and said keyed hash function is a keyed compression function f.

11. The method of claim 7 wherein said hash function is an iterated hash function F and said keyed hash function is an iterated hash function F.

12. The method of claim 7 further comprising the steps of:

using a result from said keyed hash function to produce a message authentication code; and

sending said message authentication code in association with said message for authenticating said message using said message authentication code.

13. The method of claim 7 further comprises:

using a result from said keyed hash function to produce a message authentication code; and

comparing said message authentication code to a received message authentication code received with said message, whereby said message is authentic if said message authentication code and said received authentication code match.

14 A message authentication system comprising:

processing circuitry configured to perform a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function and to use a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function.

15. The system of claim 14 wherein said processing circuitry configured to provide a first portion and a second portion of said message, perform a hash function using said first portion as an input to achieve a result, and perform a keyed hash function using said second portion and said result as inputs.

16. A message authentication system comprising:

processing circuitry configured to provide a first portion and a second portion of said message, perform a hash function using said first portion as an input to achieve a result, and perform a keyed hash function using said second portion and said result as inputs.

17. The system of claim 16 wherein said processing circuitry configured to determine whether said message fits within an input block of a compression function.

18. The system of claim 17 wherein said processing circuitry configured to perform a single iteration of a compression function using a key and said message as inputs when said message fits within an input block of said compression function.